frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 20 March 2024
DOI 10.3389/fenrg.2024.1383090

OPEN ACCESS

EDITED BY
Haris M. Khalid,
University of Dubai, United Arab Emirates

REVIEWED BY
Nishant Kumar,
Indian Institute of Technology Jodhpur, India
Kenneth E. Okedu,
Melbourne Institute of Technology, Australia

*CORRESPONDENCE
Mouloud Aoudia,
mouloud.aoudia@nbu.edu.sa

RECEIVED 06 February 2024
ACCEPTED 06 March 2024
PUBLISHED 20 March 2024

CITATION
Iftikhar H, Khan N, Raza MA, Abbas G, Khan M, Aoudia M, Touti E and Emara A (2024), Electricity theft detection in smart grid using machine learning.
Front. Energy Res. 12:1383090.
doi: 10.3389/fenrg.2024.1383090

Electricity theft detection in smart grid using machine learning

Hasnain Iftikhar[1,2], Nitasha Khan[3], Muhammad Amir Raza[4], Ghulam Abbas[5], Murad Khan[6], Mouloud Aoudia[7]*, Ezzeddine Touti[8,9] and Ahmed Emara[10,11]

[1]Department of Mathematics, City University of Science and Information Technology, Peshawar, Khyber Pakhtunkhwa, Pakistan, [2]Department of Statistics, Quaid-i-Azam University, Islamabad, Pakistan, [3]British Malaysian Institute, Universiti Kuala Lumpur, Sungai Pusu, Malaysia, [4]Department of Electrical Engineering, Mehran University of Engineering and Technology SZAB Campus Khairpur Mir's, Sindh, Pakistan, [5]School of Electrical Engineering, Southeast University, Nanjing, China, [6]Department of Statistics, Abdul Wali Khan University, Mardan, Pakistan, [7]Department of Industrial Engineering, College of Engineering, Northern Border University, Arar, Saudi Arabia, [8]Department of Electrical Engineering, College of Engineering, Northern Border University, Arar, Saudi Arabia, [9]Department of Electrical Engineering, Higher Institute of Applied Sciences and Technology of Kasserine, University of Kairouan, Kairouan, Tunisia, [10]Department of Electrical Engineering, University of Business and Technology, Jeddah, Saudi Arabia, [11]Department of Engineering Mathematics, and Physics, Faculty of Engineering, Alexandria University, Alexandria, Egypt

Nowadays, electricity theft is a major issue in many countries and poses a significant financial loss for global power utilities. Conventional Electricity Theft Detection (ETD) models face challenges such as the curse of dimensionality and highly imbalanced electricity consumption data distribution. To overcome these problems, a hybrid system Multi-Layer Perceptron (MLP) approach with Gated Recurrent Units (GRU) is proposed in this work. The proposed hybrid system is applied to analyze and solve electricity theft using data from the Chinese National Grid Corporation (CNGC). In the proposed hybrid system, first, preprocess the data; second, balance the data using the k-means Synthetic Minority Oversampling Technique (SMOTE) technique; third, apply the GTU model to the extracted purified data; fourth, apply the MLP model to the extracted purified data; and finally, evaluate the performance of the proposed system using different performance measures such as graphical analysis and a statistical test. To verify the consistency of our proposed hybrid system, we use three different ratios for training and testing the dataset. The outcomes show that the proposed hybrid system for ETD is highly accurate and efficient compared to the other models like Alexnet, GRU, Bidirectional Gated Recurrent Unit (BGRU) and Recurrent Neural Network (RNN).

KEYWORDS

electricity theft detection, anomaly detection, smart grid, machine learning, economic development

1 Introduction

Electric energy is a fundamental requirement for daily life activities and processes in the modern world. Using energy resources is essential for the economic development and growth of every country worldwide (Lowitzsch et al., 2020). However, crises can arise when energy consumption exceeds production, leading to a shortfall and interruption in energy supplies (Ren et al., 2021). Many underdeveloped and economically unstable countries, including the India, Indonesia, Malaysia, Pakistan, Nigeria, Ethopia and China, are currently facing energy crises (Østergaard et al., 2021). Electricity is one of the primary

forms of energy used globally, and the demand for it is rapidly increasing. However, many developed and developing countries face electricity crises due to Technical Losses (TL) and Non-Technical Losses (NTLs) (Kumar et al., 2019). NTLs are caused by fraud, electricity theft, tampering with the recording process, and non-billing of electricity (Rahman et al., 2020). To mitigate NTLs, modern methods for detecting fraud and electricity theft are required. NTLs are the primary cause of revenue loss in smart grids (Stracqualursi et al., 2023). Recent studies have revealed that NTLs result in global annual losses of USD 89.3 billion in the utility sector of electrical energy (de Souza et al., 2020). The problem of NTLs is still relevant in both developed and developing countries. Normally, energy losses in developed countries range between 0.5% and 3% yearly in revenue collection (Park and Kim, 2020; Kumar et al., 2020). In developing countries, the losses are approximately 4.5 billion USD annually, accounting for about 50% of electricity produced (Quasim et al., 2023). Developed countries like the United Kingdom (UK) and the United States of America (United States of America) face annual losses ranging from 1 to 6 billion USD (Duarte Soares et al., 2022). Pakistan also faces NTLs of 0.89 billion USD per annum due to non-billing and electricity theft (Rehan et al., 2023). NTLs can be intentional or unintentional, and many power supply companies try to detect and reduce them efficiently (Zhang et al., 2020). Due to the rise in electricity fraud, several methods have been adopted to automatically detect electricity theft, like assessing electricity consumption records (Kocaman and Tümen, 2020). Hardware and data-driven solutions are implemented to mitigate NTLs. Hardware solutions commonly use grid system variables, including power, voltage, and current, while data-driven solutions analyze and mine consumers' load profiling and other information to detect NTLs (Muzumdar et al., 2022). However, it faces many obstacles in ETD and fraudulent consumers due to its technical theft strategies, including line tapping, meter tempering, etc., and needs extra devices for implementation (Chandrasekhar et al., 2020). Hence, it is costly, Furthermore, to tackle the NTLs and ETD in smart grids, Advanced Metering Infrastructure (AMI) is better than old mechanical metering (Saxena et al., 2021).

Due to the increase in the number of electricity thieves, the electric utilities are facing problems in providing electricity to their consumers in an efficient way (Xie, 2023). An accurate ETD is quite challenging due to the inaccurate classification on the imbalance electricity consumption data, the overfitting issues and the high false positive rate of the existing techniques (Blazakis et al., 2020). Therefore, intensified research is needed to accurately detect the electricity thieves and to recover a huge revenue loss for utility companies. To address the above limitations, this paper presents a new model, which is based on the supervised machine learning techniques and real electricity consumption data.

In this study, we propose a new hybrid system based on deep learning models that accurately detect electricity theft in smart grids while also being efficient. The first step involves preprocessing the data and replacing the missing values using a simple imputer method. Next, we use the standard-scalar approach to execute a min-max operation for data normalization. After data preparation is finished, we obtain samples for typical users. We then balance the data using k-means SMOTE to create samples for fraudulent users by altering honest samples with current theft attacks. In the third step, the balanced data from the previous stage is used for classification purposes. The MLP and GRU modules were created in Python® using balanced smart meter data and supplementary data as input for prediction. We apply efficient performance criteria in the final phase to investigate the results. To validate the proposed model's performance using various performance measures, including accuracy, F1-score, precision, and recall. In addition, we also test the consistency and efficiency of the trained model on new samples in the second phase to identify whether the new sample belongs to the honest class or the malicious. The main applications of this paper are: the proposed approach provides the solution for the problem present in the power sector, such as to wastage of electrical power due to electricity theft. This model can efficiently be applied by the utility companies using the real electricity consumption data to identify the electricity thieves and reduce the energy wastage and finally, the proposed approach can be used against the all types of consumers who steal the electricity.

The key contributions of this paper: A comprehensive data pre-processing is performed using interpolation, three sigma rule, and normalization methods to deal with missing values and outliers in the dataset. The data pre-processing step gives the refined input, which improves the performance of the classifier. A class balancing technique, K-means SMOOTHE, is proposed to address the problem of imbalance data. MLP is applied to predict final misclassification, which improves the performance along with MLP, GRU technique is utilized for efficient parameter optimization of the classifier. The complete procedure of the proposed hybrid system (MLP-GRU) for ETD is: first, preprocess the data; second, balance the data; third, apply the GRU model to the extracted purified data; fourth, apply the MLP model to the extracted purified data; and finally, evaluate the performance of the proposed system using different performance measures like a graphical analysis and a statistical test. We conduct extensive simulations on real electricity consumption data set and for comparative analysis, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), Receiving Operating Characteristics Area Under Curve (ROC-AUC), and Precision Recall Area Under Curve (PR-AUC) are used as performance metrics.

The rest of the article is organized as follows: Section 2 contains the existing literature and Section 3 consists of a proposed hybrid system. Section 4 discusses the results and compared the results with the best studies available in literature. Finally, Section 5 presents a conclusion and directions for future research work.

2 Review of existing literature

The problem of ETD and NTLs is rising quickly at global scale, and researchers are developing techniques to tackle this problem by applying statistical, machine learning, and deep learning models (Jaiswal et al., 2020). The machine learning models, including Random Forest (RF), Decision trees (DT), Bagging Ensemble (BE), Artificial Neural Networks (ANN), and K-Nearest Neighbors (KNN), were comparatively evaluated for automated ETD in smart grid environments and found RF yields 10% more improved accuracy in ETD compared to other used methods (Zidi et al., 2023). The rapid growth in NTLs and electricity thefts are the major challenges for distribution network operators. In (Fei et al.,

2022) neural network model based on Neural Architecture Search (NAS) is developed to analyze and detect electricity theft in missing value scenarios through density-based spatial clustering of application and noise clustering technique and achieved an excellent result of AUC of 0.926 in the NTLs and ETD. The authors in (Banga et al., 2022) used different deep learning models for NTLs and ETD, including GRU, Long Short-Term Memory (LSTM) models, MLP, and Convolutional Neural Networks (CNN). However, these models lack efficient hyper parameter tuning, which leads to poor generalization for tackling these issues.

The researchers in (Asif et al., 2022) proposed hybrid deep learn ing models based on Bidirectional Long Short-Term Memory (Bi-LSTM) networks and Two-Dimensional Convolutional Neural Networks (2D-CNN) to detect NTLs in smart meters, and they outperformed other methods with ROC 0.97 and AUC 0.98 in smart meters data. In detecting NTLs and ETD, the problem of class imbalance, the curse of dimensionality reduction, and inappropriate tuning of hyper parameters arise in commonly used machine learning and deep learning models. Therefore, to cope with these problems, the authors in (Ullah et al., 2022) proposed a hybrid deep learning method based on Alexnet and Adaboost for ETD in smart grids. They achieved the best performance results compared to other methods used, and the problem of class imbalance and the curse of dimensionality is being tackled by under-sampling techniques and tuning hyper parameters by the Artificial bee Colony (ABC) optimization algorithm. Furthermore, the authors in (Kumar et al., 2022) proposed a hybrid method based on CNN and RF to predict ETD in power grids accurately. The RF is employed for classification, while CNN efficiently extracts the potential features. A deep learning-based hybrid model is designed by (Hasan et al., 2019), which uses the pros of both CNN and LSTM models and efficiently extracted the hidden patterns and temporal correlation in ETD of consumers in smart grid systems, respectively. The researchers in (Gupta et al., 2022) proposed a Deep Neural Network (DNN) model, first they resolved the dimensionality problem, and then important features were selected for the detection of fraud in the electricity consumption of the smart grid. The ETD results show the proposed method's best performance over the other used models. The problem of diverse theft patterns in electricity consumption due to a significant class imbalance in data leads to higher false positive rates, and ensemble models fail to detect NTLs. Hence, the authors in (Alameady et al., 2022) tried to overcome this issue by proposing hybrid neural networks named MLP-GRU for detecting electricity thefts in smart meter data by analyzing the auxiliary information of the consumers.

With the advent of smart meters, different types of electricity theft techniques have been adopted, and their detection is very difficult using conventional methods. The researchers in (Li et al., 2019) designed a statistical and machine learning-based Internet of Things (IoT) system to identify and notify electricity consumers about electricity thefts. Many studies based on data-driven techniques have been used for NTLs identification in the literature. Most studies have focused on boosting approaches, and less attention is given to bagging approaches like Extra Trees (ET) and RF (Siu et al., 2022). Furthermore, commonly used machine learning models such as Support Vector Machine (SVM) and neural networks yield a higher false positive rate and a lower detection rate in ETD (Ahir and Chakraborty, 2022). The authors in (Gong et al., 2020) have explored a Conditional Variation Auto-Encoder (CVAE) combined with CNN for extracting relevant features from high-dimensional data and presented a solution to the problem of data augmentation. Furthermore, many studies and experiments have been conducted on ETD in AMI through machine learning techniques (Aziz et al., 2020). The researchers in (Jokar et al., 2015) implemented a pattern recognition technique based on unsupervised learning models for ETD in the data set of smart meters.

The deployment of advanced sensors has strengthened the monitoring capability of power plants. In the context of the cogeneration process, the plant cooling is performed by the cooling towers using the condensation process on exhaust steam. However, the computer networks and industrial control systems built on this sensor-based digital layer may become vulnerable to cyber attacks. This may eventually raise a concern on the performance and security of these energy utilities. To resolve this issue, an inoculated subobserver-based fusion filter is proposed. It improves the resilience against malicious attacks in combined cycle power plants with desalination units, which are usually functioning in a closed-loop environment and infected with injected attacks. A time-delay-based state representation is considered for the system (Khalid et al., 2019).

IoT is a developing technology that provides the simplicity and benefits of exchanging data with other devices using the cloud or wireless networks. However, the changes and developments in the Internet of Things (IoT) environment are making IoT systems susceptible to cyber attacks which could possibly lead to malicious intrusions. The impacts of these intrusions could lead to physical and economical damages. This article primarily focuses on the IoT system/framework, the IoT, learning-based methods, and the difficulties faced by the IoT devices or systems after the occurrence of an attack. Learning-based methods are reviewed using different types of cyber attacks, such as denial-of-service (DoS), distributed denial-of-service (DDoS), probing, user-to-root (U2R), remote-to-local (R2L), botnet attack, spoofing, and man-in-the-middle (MITM) attacks (Inayat et al., 2022).

Synchrophasor-based wide-area monitoring system (WAMS) applications are vital for acquiring the real-time grid information under ambient and nonlinear conditions. The high dependence on sensor data and signal-processing software for daily grid operation is becoming a concern in an era prone to cyberattacks. To resolve this issue, a mixture density-based maximum likelihood (MDML) estimation was proposed to detect attack vectors. The algorithm was deployed at each monitoring node using a track-level fusion (TLF)-based architecture. A parallelized message passing interface (MPI)-based computing was processed to reduce its computational burden. This work adopted a mature application known as oscillation detection as an example of a monitoring candidate to demonstrate the proposed method (Khalid et al., 2023).

This paper introduces the theft detection method which uses comprehensive features in time and frequency domains in a deep neural network-based classification approach. We address dataset weaknesses such as missing data and class imbalance problems through data interpolation and synthetic data generation processes. We analyze and compare the contribution of features from both

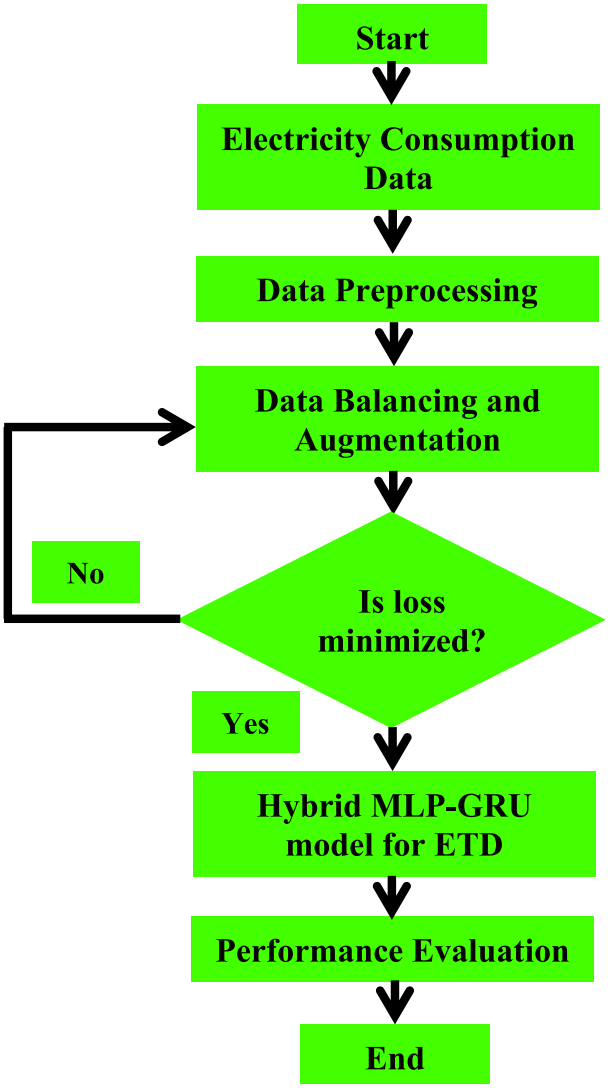

FIGURE 1
Flow chart of the proposed model for ETD.

time and frequency domains, run experiments in combined and reduced feature space using principal component analysis and finally incorporate minimum redundancy maximum relevance scheme for validating the most important features. We improve the electricity theft detection performance by optimizing hyper-parameters using a Bayesian optimizer and we employ an adaptive moment estimation optimizer to carry out experiments using different values of key parameters to determine the optimal settings that achieve the best accuracy (Lepolesa et al., 2022).

This work proposes two novel methods to resolve the above-mentioned issues: Tomek Link Borderline Synthetic Minority Oversampling Technique with Support Vector Machine (TBSSVM) and Temporal Convolutional Network with Enhanced Multi-Layer Perceptron (TCN-EMLP). The former resamples the data by balancing the majority and minority class instances. Whereas, the latter classifies normal and fraudulent consumers. Moreover, deep learning models suffer from high variance in their final results due to the assignment of different weights. Therefore, an averaging ensemble strategy is applied in this work to reduce the high variance (Arif et al., 2022).

In previous literature, most research focused on non-malicious electricity consumption patterns and showed low detection rates for NTLs. In (Ding et al., 2019), the authors proposed a hybrid approach based on the enhanced internal structure of the LSTM model with a combination of the Gaussian Mixture Model (GMM). However, it only applies to low-dimensional data and is not robust to outliers. In further studies (Jindal et al., 2016), a hybrid method based on SVM has been proposed for detecting fraudulent consumers but has not shown an effective performance in the overall technical evaluation. The authors (Kabir et al., 2022; Kumari et al., 2022) proposed a hybrid deep learning model based on Multi-Layer Perceptron (MLP) and Gated Recurrent Unit (GRU) for the detection of electricity thefts and NTLs in smart meter data. The MLP network is used for analyzing non-malicious factors on auxiliary information in the daily consumption of electricity data, while the GRU network is used for analyzing smart meter data. Furthermore, a random search algorithm turns hyper-parameters and performs better than other methods.

3 Research method

In this section, we discuss in detail the complete procedure of the proposed hybrid system for ETD. To do this, first, preprocess the data; second, balance the data; third, apply the GRU model to the extracted purified data; fourth, apply the MLP model to the extracted purified data; and finally, evaluate the performance of the proposed system using different performance measures like a graphical analysis and a statistical test. The framework of proposed method is given in Figure 1.

3.1 Preprocessing of raw data

In this work, the proposed hybrid system is applied to the electricity consumption data from the CNGC dataset, which is both authentic and accessible. The dataset contains 42,372 records of total consumer, of which 38,752 are honest and share information on regular basis, and 3615 are records of theft consumers. The dataset's sample interval is set to once per day. The entire electricity consumption value is represented in the dataset as rows, while the electricity consumption value for a certain day is provided as a column. Moreover, statistics are gathered during onsite inspections. However, the electricity consumption dataset comprises outliers, missing values, and extremely dispersed data. These irregularities must be corrected before developing the ETD model. Preprocessing is necessary in this case to recover the missing values, reduce the outliers, and normalize the data within a certain range. The entire amount of consumer data was 42,372 before pre-processing; however, five rows were eliminated by the Simple Imputer (SI) approach after preprocessing since all of the data in such rows were missing values. When this occurs, the SI is unsure of the value that should be ascribed. If the imputer discovers at least one actual value in the targeted record, it will impute some values rather than delete them. It is also crucial to keep in mind that the SI method operates column-wise, therefore you must transpose your data before using

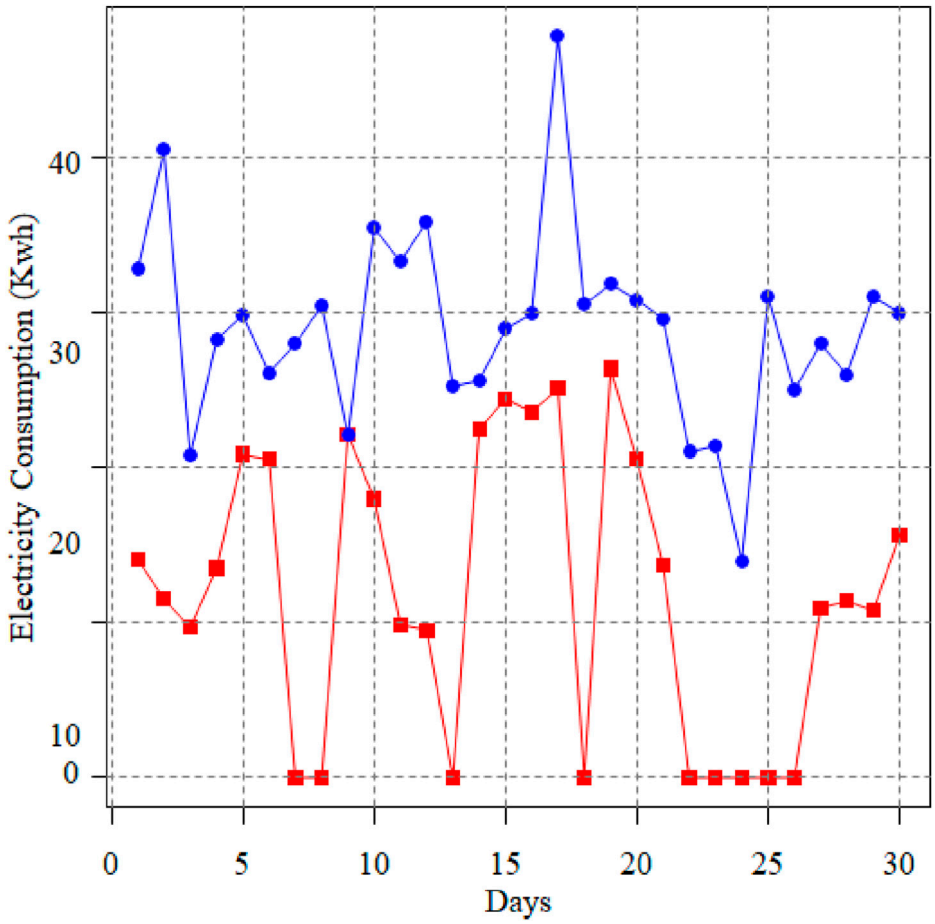

FIGURE 2
EC Pattern of honest (blue) and dishonest (red) customers.

the imputer approach. Take the data's transposition once more after imputation to return it to its original shape. The electricity consumption patterns of two consumers, the dishonest consumer, and the honest consumer, are shown in Figure 2. It demonstrates that the electrical thief has irregular electricity consumption patterns and that meter manipulation caused its electricity consumption value to decrease. In contrast, an unbiased consumer displays typical electricity consumption patterns.

3.2 Data balancing and augmentation using K means SMOOTE

Once the data set has been cleaned, the next step is to balance the data set. In this regard, there are fewer dishonest users' consumption samples in the real world. It is an unbalanced dataset, and the machine learning, deep learning, or hybrid models during training are biased toward the majority of class samples. Moreover, they neglect occurrences of minority classes that affect performance. Numerous resampling approaches have been presented in the literature to address this issue (Chung, 2014; Zheng et al., 2017; Ding et al., 2019). To do this, the k-means SMOTE algorithm and augmentation techniques are combined in this study to simultaneously over and under sample data classes to address the imbalance problem. Removing the majority of class links until both classes have an equal number of entities achieves the stated goal. The pseudo-code of the k-means SMOTE algorithm is given in Table 1, and an example of synthetic data generation through k-means SMOTE can be seen in Figure 3.

3.3 The proposed model

After the data set has been cleaned and balanced, the next step is to model the purified data set. To this end, within the proposed hybrid system, we combine the features of MLP and GRU models to obtain a new hybrid deep learning model. The GRU network uses smart meter data from the CNGC dataset as input, and the MLP network observes ancillary data with techniques that explore non-harmful elements within electricity consumption data. The details about the GRU, MLP, and the proposed hybrid model (GRU-MLP) are in the following subsections.

3.3.1 Gated recurrent unit

In general, it can be noticed that electricity consumption patterns fluctuate a lot more than those of regular consumers. To

TABLE 1 Pseudo-code of the k-means SMOTE algorithm.

K-means SMOTE technique
Inputs:
Minority class samples Xmin
Number of nearest neighbors K
Output:
Synthetically generated minority class samples (Xsyn)
Cluster the minority class samples Xm in using the K-means algorithm with K clusters
Let C1, C2,. and CK be the resulting clusters
For each cluster Ci: a. Find the k-nearest neighbors of each sample in Ci using a distance metric (e.g., Euclidean distance). Let NNi denote the set of nearest neighbors of Ci.
b. For each sample in Ci, randomly select one of its k nearest neighbors from NNi and generate N/K synthetic samples by interpolating between the sample and its selected neighbor. Add the synthetic samples to the set (Xsyn)
c. Return the set of synthetically generated minority class samples (Xsyn)

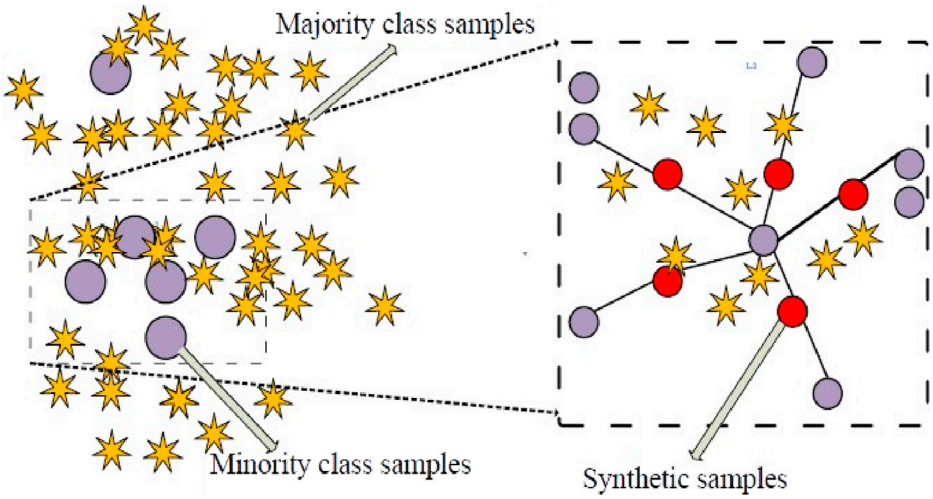

FIGURE 3
Synthetic data generation through k-means SMOTE.

identify co-occurring connections in time series data, 1D data is supplied into the GRU model. To identify comparable dependencies in time series data, Chung et al. presented the GRU algorithm in (Ding et al., 2019). It features memory modules to store significant periodic patterns, which aids in managing unexpected variations in electricity consumption patterns brought on by regular occurrences like varying weather conditions, large home parties, weekends, etc. Moreover, it addresses the vanishing gradient issue with RNN. LSTM and GRU are regarded as RNN variations. The effectiveness of LSTM and GRU with an RNN model on various sequential datasets is compared by the authors in (Buzau et al., 2019). The vanishing gradient issue of the RNN is resolved by both models, which outperform it. The authors in (Aslam et al., 2020) conduct comprehensive tests on 10,000 RNN and LSTM designs. Their final experimental findings demonstrate that GRU is the only model that outperforms all others. Based on the analysis above, we chose GRU to extract the best features from the electricity consumption dataset because it performs well on sequential datasets. It has gates for resetting, updates and regulate the data that moves inside the network. The update gate determines how much historical data should be kept for decision-making in the future. Conversely, the reset gate determines how much historical data should be retained or deleted. Update and reset gate equations are related to one another. Yet, the use of weights and gates accounts for the distinction. The GRU model's mathematical Eqs 1–4 (Kabir et al., 2021) are provided below:

$$z_t = \sigma(W_Z, [h_{t-1}, x_t]) \quad (1)$$

$$r_t = \sigma(W_r, [h_{t-1}, x_t]) \quad (2)$$

$$\hat{h}_t = tanh(W, [r_t * h_{t-1}, x_t]) \quad (3)$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * \hat{h}_t \quad (4)$$

In these equations, update gate z_t controls the extent to which states information from the previous moment is substituted into the

TABLE 2 Pseudo-code of the MLP-GRU technique.

Algorithms of the proposed hybrid (MLP-GRU) model
Inputs:
SGCC dataset with features X and labels y
Number of epochs n–epochs
Batch size batch–size
Learning rate lr
Number of GRU units n–units
Number of MLP layers n–layers
Dropout rate dropout–rate
Output:
Trained MLP-GRU model with confusion matrix
Split the CNGC dataset into training, validation, and testing sets

current state, and reset gate r_t controls the extent to which state information from the previous moment is ignored. σ is the activation function. The candidate activation h_t, is computed with the reset gate r_t (which control how much of the previous information needs to be retained), and $*$ denotes the element wise multiply operation. Finally, h_t, represents the actual activation of the proposed GRU unit at time t, which is a linear interpolation between the previous activation h_{t-1}, and the candidate activation h_t,.

3.3.2 Multi-layered perceptron network

The MLP network is used to evaluate the auxiliary dataset. There are multiple layers of hidden neurons in the MLP. These hidden layers in the MLP network are selected using the validation dataset.

$$H_n = \sigma\left(\sum U_{i,n} * X_i + B_n\right) \tag{5}$$

"Where", $i = 1, 2, 3, \ldots .N$,

$$Y_n = \sigma\left(U_n * H_{n-1} + B_n\right) \tag{6}$$

Eq. 5 specify that U_n refers to the weights of layer n, H_{n-1} for the input layer's prior hidden states, and B_n for the bias. The activation function, which activates the neuron, is called after the input values have been processed, and it decides whether or not to pass the values to the subsequent layer. The sigmoid activation function is represented by σ. The output layer, designated as Y_n, is shown in Eq. 6. In this study, the final output layer was activated using a sigmoid activation function for the binary classification, while the hidden layer was activated using the Rectified Linear Unit (ReLU) (Mukhopadhyay, 2019). Using a batch normalization layer to normalize the input values sped up the network convergence. A dropout layer was then included as a regularization method to avoid overfitting.

3.3.3 Hybrid MLP-GRU model

The hybrid neural network composed of MLP and GRU is introduced in the proposed work. Electricity consumption data is used as input into the proposed GRU-MLP network. The proposed methodology was motivated by research for identifying electricity theft done in (Cheng et al., 2021). The research in (Xu et al., 2018) generated the LSTM-MLP hybrid neural network classifier. The GRU module with 100 neurons receives the preprocessed smart meter energy consumption data. The number of neurons in the GRU layer is two times higher than in the MLP model. The GRU layer generalizes the embedding at a lower computational cost with comparatively fewer cells. Since the data includes low-dimensional features, auxiliary data with 20 neurons is sent as input to the MLP module. The data is normalized using the batch normalization approach until submitted to the final dense layer. The final layer has just one neuron with a sigmoid activation mechanism. The pseudo-code of the MLP-GRU technique is given in Table 2. On the other hand, an overview of the proposed hybrid system can be seen in Figure 4.

Initialize the MLP-GRU model:

a. Create an MLP with n–layers fully connected layers and Rectified Linear Unit (ReLU) activation function. Each layer should have dropout rate.
b. Create a GRU layer with n–units hidden units and a sigmoid activation function.
c. Concatenate the output of the MLP and the GRU layer.
d. Add a final fully connected layer with a sigmoid activation function.

Train the MLP-GRU model:

a. Define the binary cross-entropy loss function and the Adam optimizer with learning rate.
b. Train the model for n-epochs with a batch size of batch-size.
c. Evaluate the model on the validation set after each epoch and save the best model.

The training, validation, testing and best performance data for MLP-GRU model for theft detection is given in Figure 5.

3.4 Benchmark models

In this section, we explore some standard existing models that are compared with the proposed hybrid model, such as Alexnet, GRU, BGRU, and RNN as follows:

1. Alexnet: It is a deep CNN architecture that is widely recognized as one of the key break throughs in the field of computer vision and deep learning, as it achieved a significant improvement in image classification accuracy on the ImageNet dataset. The AlexNet architecture consists of five convolutional layers, followed by three fully connected layers and a final softmax layer for classification. It also incorporates several novel techniques, including ReLU as activation functions, data augmentation through image mirroring and cropping, and dropout regularization to prevent overfitting. One of the major contributions of AlexNet was demonstrating the effectiveness of deep learning for image recognition tasks and paving the way for subsequent advances in the field. Many state-of-the-art CNN architectures build on the foundations laid by AlexNet and continue to push the

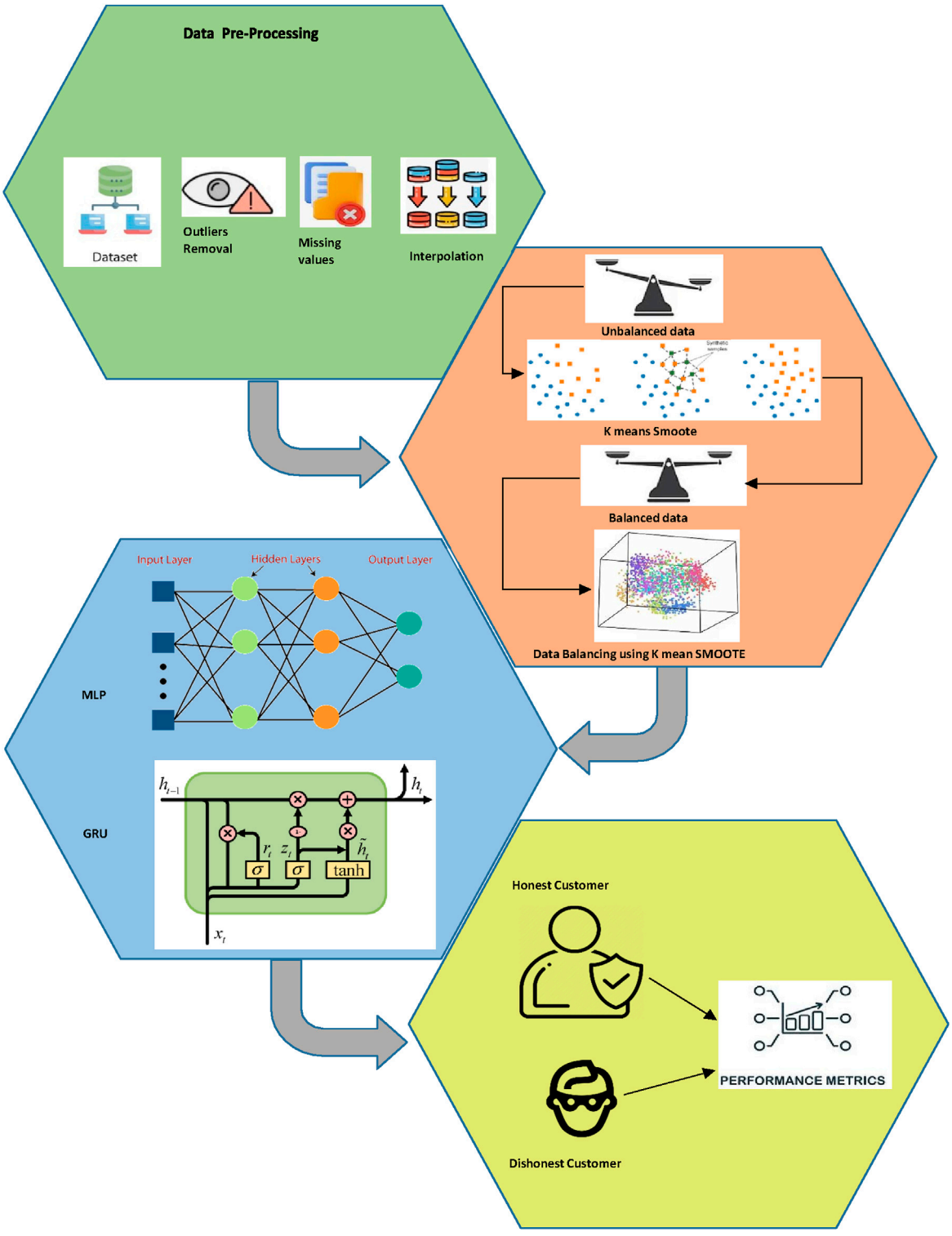

FIGURE 4
An overview of the proposed hybrid system.

boundaries of image recognition and other computer vision tasks (Khan et al., 2024).

2. GRU: It is a type of RNN architecture that addresses the vanishing gradient problem and allows for capturing long-term dependencies in sequential data. It was introduced as an alternative to the traditional Long Short-Term Memory (LSTM) units, offering a simpler and more computationally efficient design. GRU units consist of update and reset gates, which control the flow of information within the network. The update gate determines how much of the previous hidden state

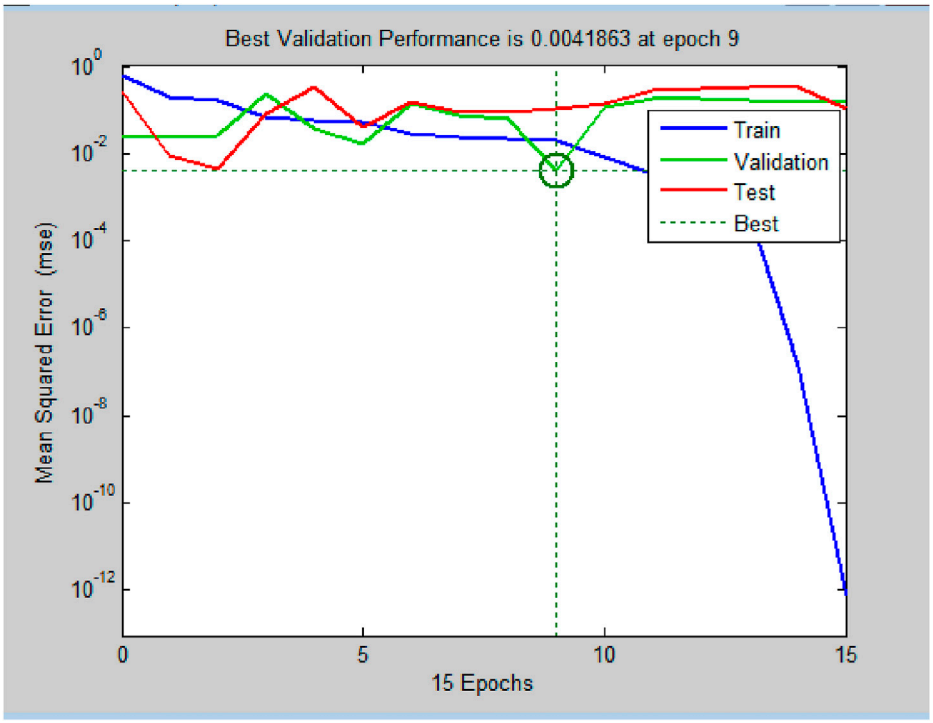

FIGURE 5
Performance graph showing the training, validation, testing and best performance after nine epochs for MLP-GRU model.

should be retained and how much of the new input should be added. The reset gate helps the network decide how much of the previous hidden state is relevant for the current input. These gates enable GRUs to selectively update and reset their hidden state based on the input sequence, allowing them to capture both short-term and long-term dependencies. One advantage of GRUs over LSTMs is their simplified architecture, which leads to faster training times and requires fewer parameters. This can be particularly beneficial when dealing with large datasets or limited computational resources. Additionally, GRUs have shown comparable performance to LSTMs on various tasks, such as language modeling, speech recognition, machine translation, and sentiment analysis. The GRU technique has proven effective in modeling sequential data due to its ability to handle both short-term and long-term dependencies. It has been widely adopted in various fields, including natural language processing, time series analysis, and sequential data generation. Researchers and practitioners continue exploring and refining GRU-based models, exploring variations and combining them with other techniques to improve their performance and accuracy (Munawar et al., 2021).

3. BGRU: It is also a deep learning architecture commonly used for sequential data modeling, such as text, speech, and time series data. It is an extension of the standard GRU architecture incorporating bidirectional processing, allowing the network to learn from past and future input sequences. The architecture consists of two parallel GRU layers, one processing the input sequence in a forward direction and the other in a backward direction. The outputs of these two layers are then concatenated and passed through a dense layer for classification or regression. BGRU is particularly useful for applications where context information from past and future input sequences is important, such as in natural language processing tasks like sentiment analysis, named entity recognition, and machine translation. BGRU has been shown to achieve stateof-the-art performance on a wide range of tasks and is often used as a baseline model for comparison with more complex architectures. Overall, BGRU is a powerful and versatile deep-learning technique for sequential data modeling that has become increasingly popular recently. The RNNs are deep learning models commonly used for sequential data processing, such as text, speech, and time-series data. Unlike traditional neural networks that take fixed-size inputs and produce fixed-size outputs, RNNs are designed to operate on variable length sequences. They achieve this by including loops within the network that allow information to persist over time. This makes them particularly effective at processing inputs that have a temporal or sequential nature (Gul, 2020).
4. RNN: The basic RNN architecture consists of a single recurrent layer that processes input sequences one element at a time while maintaining a hidden state that captures the network's internal representation of the input sequence up to that point. However, standard RNNs can suffer from the vanishing gradient problem, making it difficult to learn long-term dependencies in the data. More advanced RNN architectures have been developed to address this issue, including LSTM and GRU networks. These architectures incorporate specialized gating mechanisms that allow the

network to selectively remember or forget information over time, making them more effective at processing longer input sequences. RNNs have shown impressive results in various applications, including natural language processing, speech recognition, and time-series forecasting (Bohani et al., 2021).

3.5 Performance matrix

This section provides an in-depth analysis to evaluate the proposed hybrid system performance with that of the considered benchmark models. In this study, accuracy, F1-score, precision, recall, and Matthews' correlation coefficient (MCC) are performance indicators used to verify the effectiveness of the proposed techniques. These are derived from the confusion matrix parameters True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN), which, respectively, reflect the ratio of consumers who are classified as honest consumers correctly, incorrectly as normal consumers, fraudulent users correctly, and users incorrectly classified as fraudulent users. One of the most frequently used measures to show the model's percentage of precise prediction is accuracy. The mathematical Eq. 7 for the accuracy is given by (Zidi et al., 2023):

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FN} \tag{7}$$

Increasing the True Positive Rate (TPR), Fraud Detection Rate (FDR), and low false positive rate is the main goal of ETD (Jindal et al., 2016). To detect NTLs using binary classification, the ROC-AUC is a suitable metric. To create it, TPR, also known as recall, is plotted against false positive rate while the decision thresholds are being adjusted. The range of the score is 0–1. In the event of a class imbalance issue, it is a more precise measurement. False positive rate and TPR are helpful metrics for evaluating a model's effectiveness at detecting NTLs, but they do not account for precision. Hence, PR-AUC is a helpful metric that is also an appropriate measure for imbalanced datasets to assess the model's precision. Thus, the mathematical form for the precision, recall, F1-score, and MCC are given in Eqs 8–11 (Razavi et al., 2019).

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$Precision = \frac{TP}{TP + FP} \tag{9}$$

$$F1\,Score = 2*\frac{Precision*Recall}{Precision + Recall} \tag{10}$$

$$MCC = \frac{TP*TN - FP*FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{11}$$
$$j$$

In contrast to performance measures, to assess the significance of the differences in the prediction performance of the proposed models, the Diebold and Mariano Test (DMT) was performed (Meidan et al., 2020). The DMT is a widely used statistical test for comparing predictions obtained from different models. To assess whether the prediction accuracy of the proposed prediction model is significantly better than that of benchmark models, DMT statistic was introduced in this study, as determined by the Eq. 12:

TABLE 3 Hyper parameters of MLP-GRU.

Hyper parameters	Values
Epoch	30,50
Batch size	32,64
Optimizer	Adam, adammax, SGD
Dropout	0.3,0.2,0.5,0.01,0.1
Activation	Relu, elu, sigmoid

$$D = \frac{x}{\sqrt{V(\bar{x})}} \tag{12}$$

Where; $\bar{x} = \frac{1}{t}\sum_{n=1}^{t} x_n$, $x_n = (z_n - \tilde{z}_{1n})^2 - (z_n - \tilde{z}_{2n})^2$,

$$V(\bar{x}) = \frac{1}{t}\left(2\sum_{j=1}^{t-1} r_j + r_0\right), \text{and } r_j = cov\left(x_n - x_{n-j}\right)$$

$\tilde{z}_{1n}$ is the predicted value of the first predictive model and $\tilde{z}_{2n}$ is the predicted value of the second predictive model at time n. If the DMT statistic is negative, the first predictive model is statistically better than the second predictive model.

4 Results and discussion

Real-time consumer data for residential customers makes up the exploited data. The customers are divided into two groups based on similar indexing patterns and appropriately designated consumption categories. Each consumer's consumption pattern is represented by a staging numeric binary. Label 0 denotes an honest consumer, while label 1 denotes a dishonest one. Each consumer's tracked and reordered patterns are collected every 24 h. For each of the theft versions, benign class data is modified to create harmful data. Data from both types is later combined. Due to the model's deviation towards the majority class, a data balancing strategy is necessary to minimize the class bias issue. The data is balanced using K-means SMOTE. The hyper-parameters and their appropriate values obtained during the tuning of the proposed MLP-GRU model are shown in Table 3. Due to their lengthy computation, we investigate fewer hyper-parameters.

The proposed model's training process is handled by the epoch variable. We accomplish 15 iterations, or epochs, of our model. The results show that the MLP-GRU's training accuracy (accuracy on seen data) gradually improves with each iteration, reaching a maximum of 86% in the last iteration. Whereas the MLP-GRU accuracy gradually rises as well, reaching 88% at the final iteration when utilizing the testing data (accuracy using unseen data). The CNGC dataset has some zero values, which makes it difficult for the proposed classifier to learn it correctly in the early iterations. As a result, during the first three epochs, training accuracy is higher than testing accuracy, indicating that overfitting has taken place. The suggested model successfully learns the zero values after the third iteration and the overfitting problem is fixed. At various iterations, the MLP-GRU loss is also calculated and recorded. The training loss is decreasing with each iteration, until it achieves a minimum of 0.108 at the 10th iteration. The testing loss also decreases until the

10.3389/fenrg.2024.1383090

TABLE 4 Performance measures of the proposed MLP-GRU with various training and testing case.

Case 1: 50% training and 50% testing set.								
Methods	Recall	Precision	F1-Score	Accuracy	Test loss	AUC	ROC	MCC
MLP-GRU	90	87	89	87.80	32	91	100	73
Alexnet	85	96	90	87.63	34	94	85	73
BGRU	89	82	86	83.55	38	88	82	66
RNN	89	82	85	83.13	35	91	89	65
GRU	75	86	80	74.98	49	85	75	46
Case 2: 75% training and 25% testing set.								
Methods	Recall	Precision	F1-Score	Accuracy	Test loss	AUC	ROC	MCC
MLP-GRU	95	95	91	92.12	19	93	100	76
Alexnet	94	92	93	91.01	20	90	97	82
BGRU	89	73	80	78.24	46	84	80	57
RNN	87	87	87	84.39	35	91	88	66
GRU	82	89	85	81.57	39	90	80	60
Case 3: 90% training and 10% testing set.								
Methods	Recall	Precision	F1-Score	Accuracy	Test loss	AUC	ROC	MCC
MLP-GRU	95	94	94	93.33	20	95	100	85
Alexnet	94	86	90	89.12	22	94	95	78
BGRU	92	80	85	82.46	37	90	85	64
RNN	93	70	80	78.30	68	88	86	59
GRU	88	86	87	83.86	37	89	80	64

final iteration, when it hits 0.080. Due to the zero values included in the dataset, the model overfits during the first three iterations. After the third iteration, the model has learned both the dataset and the zero values, which eliminates the overfitting problem. Finally, the proposed model's training and testing accuracy leads to the conclusion that it generalizes effectively and avoids overfitting.

Using the same dataset, we trained the Alexnet, BGRU, and RNN models to compare our proposed hybrid model (MLP-GRU) to benchmark methods. Hence, Table 4 displays the performance measures and PR-AUC for the MLP-GRU, Alexnet, BIGRU, and RNN models in three training and testing sets cases. In the first case of 50% training and 50% testing, the proposed MLP-GRU produced recall 90, precision 87, F1-Score 89, accuracy 87.80, test loss 32, AUC 91, ROC 100, and MCC 73, respectively. Meanwhile, Alexnet produces recall 85, precision 96, F1-Score 90, Accuracy 87.63, test loss 34, AUC 94, ROC 85, MCC 73, and GRU poorly performed with recall 75, precision 86, F1-Score 80, Accuracy 74.98, test loss 49, AUC 85, ROC 75, and MCC 46, respectively. Moreover, in the second case of 75% training and 25% testing, the proposed model yields recall 95, precision 95, F1-Score 91, accuracy 92.12, test loss 90, AUC 93, ROC 100, and MCC 76, respectively, and Alexnet yields the second-best results with recall, precision, F1-Score, Accuracy, Test loss, AUC, ROC, and MCC 94, 91.01, 20, 90, 97, and 82 accordingly. However, the results produced by other benchmarks were not up to par in the second case either. Similarly, the proposed models show the best performance in the third case of 90% training and 10% testing set with recall 95, precision 94, F1-Score 94, accuracy 93.33, test loss 20, AUC 95, ROC 100, and MCC 85, followed by Alexnet with recall 94, precision 86, F1-Score 90, accuracy 89.12, test loss 22, AUC 94, ROC 80, and MCC 64. Meanwhile, GRU again performed poorly with the metrics of recall 88, precision 86, F1-Score 87, accuracy 83.86, test loss 37, AUC 89, ROC 80, and MCC 64.

It is evident from the results that the proposed model outperformed other models, and Alexnet was found to be the second-best performer in all three cases because it uses a k-means smote sampling technique to balance the data. However, GRU, performs the least well among the classifiers, with an accuracy of 74.98% at a 50% training ratio. This is because GRU does not capture long-term dependencies from the huge time series data since it is based on the probability notion and employs neural network theory. Furthermore, the training using the majority of class samples makes it biased when identifying genuine incidents of electricity theft. As a result, GRU is unable to classify the vastly unbalanced dataset accurately. By achieving 87% accuracy, the Alexnet, in contrast, performs marginally better than the BGRU. Alexnet is a deep learning model that extracts hidden patterns from data

TABLE 5 Execution time of the proposed MLP-GRU with various training and testing cases.

Technique (epochs = 30)	50% training (sec)	75% training (sec)	90% training (sec)
Alexnet	88.118	125.370	136.577
MLP-GRU	106.837	147.163	167.221
GRU	182.175	239.909	665.178
RNN	185.077	239.092	248.284
BGRU	1120.171	1832.843	1921.032

TABLE 6 The results (DM statistic) using the square loss function.

Case 1: (50% training and 50% testing set)					
Models	MLP-GRU	Alexnet	BGRU	RNN	GRU
MLP-GRU	0.00	−0.49	−3.08	−3.05	−6.75
Alexnet	0.49	0.00	−2.98	−2.61	−7.11
BGRU	3.08	2.98	0.00	2.42	−8.02
RNN	3.05	2.61	−2.42	0.00	−7.49
GRU	6.75	7.11	8.02	7.49	0.00
Case 2: (75% training and 25% testing set)					
Models	MLP-GRU	Alexnet	BGRU	RNN	GRU
MLP-GRU	0.00	0.57 -	−1.13	−2.33	0.05
Alexnet	0.57	0.00	−0.11	−0.99	0.96
BGRU	1.13	0.11	0.00	−2.19	1.62
RNN	2.33	0.99	2.19	0.00	2.29
GRU	−0.05	−0.96	−1.62	−2.29	0.00
Case 3: (90% training and 10% testing set)					
Models	MLP-GRU	Alexnet	BGRU	RNN	GRU
MLP-GRU	0.00	−2.40	−2.37	−3.12	−1.13
Alexnet	2.40	0.00	2.42	1.21	2.86
BGRU	2.37	−2.42	0.00	−3.86	3.43
RNN	3.12	−1.21	3.86	0.00	4.57
GRU	1.13	−2.86	−3.43	−4.57	0.00

on power use to detect electricity thieves. It has numerous stacks of hidden layers. However, because of the thick layers, it suffers from overfitting problems. It is unable to perform well across the board. Furthermore, we have compared our proposed model concerning execution time, and it is revealed in Table 5 that the execution time of the proposed hybrid MLP-GRU is 106.837 s in the first case of 50% training, 147.163 s for 75% training, and 167.221 s in 90% training set. This indicates that the proposed model is executed in less time than other benchmark models, including GRU, BGRU, and RNN, except for Alexnet. The Alexnet model here performed best in terms of less execution time due to the issues of imbalanced binary classification; this method works better in the least possible time.

Finally, the DMT results (test statistic values) are tabulated in Table 6. This table confirms that the prediction of the proposed hybrid system demonstrated that the GRU-MLP model significantly outperformed Alexnet, GRU, BGRU, and RNN. Moving forward, the corresponding test statistical values were negative in all cases at the 5% significance level using the loss square function. In the end, the performance of the proposed MLP-GRU *versus* the baseline models is plotted in Figure 6 for all three scenarios of training and testing, such as 50%, 50%; 75%, 25%; and 90%, 10%. The first scenario (50%, 50%) of performance matrices such as recall, precision, F1-Score, accuracy, test loss, AUC, ROC, and MCC is displayed in Figure 6A. The MLP-GRU is represented by a blueviolet bar, Alexnet by a periwinkle blue bar, BGRU by a green bar, a pink bar for RNN, and GRU by a yellow bar for the first case of training and testing, respectively. Therefore, it is evident in the bar plot that the proposed MLP-GRU performed best, followed by Alexnet, and GRU showed poor performance for ET prediction in smart grids. Moreover, Figures 6B, C explore the performance of these considered models for the second (75%, 25%) and third (90%, 10%) cases of the training and testing sets. After thoroughly evaluating the displayed plots, it was concluded that the proposed MLP-GRU model outperformed their competitors in the consistent prediction of electricity thefts in smart grids. However, the Alexnet model showed the second-best results. Additionally, we have plotted level plots of DMT p-values in Figure 7 for the proposed MLP-GRU, Alexnt, BGRU, RNN, and GRU to check their significance in predicting electricity thefts. However, Figure 7A explores the p-values of the test for the first case of 50% training and 50% testing, Figure 7B displays the second of 75% training and 25% testing, and the third one is plotted in Figure 7C for 90% training and 10% testing set. It is confirmed from the plotted level plot that the proposed MLP-GRU significantly outperformed other used deep learning models in electricity theft prediction.

To evaluate the effectiveness of the proposed hybrid system for ETD by comparing its performance with other state-of-the-art methodologies reported in the literature. To achieve this, we have presented a comparison Table 7 that highlights the superiority of the proposed hybrid system compared to the best approaches reported in the literature. For instance, study (Khan et al., 2024), the proposed method used the current study dataset and obtained performance measures [accuracy (91%), precision (97.96%), and area under curve (91.68%)] that were comparatively higher than our proposed hybrid technique [accuracy (93.3%), precision (97.5%), and area under curve (95%)]. In another study, (Munawar et al., 2021), the best-proposed

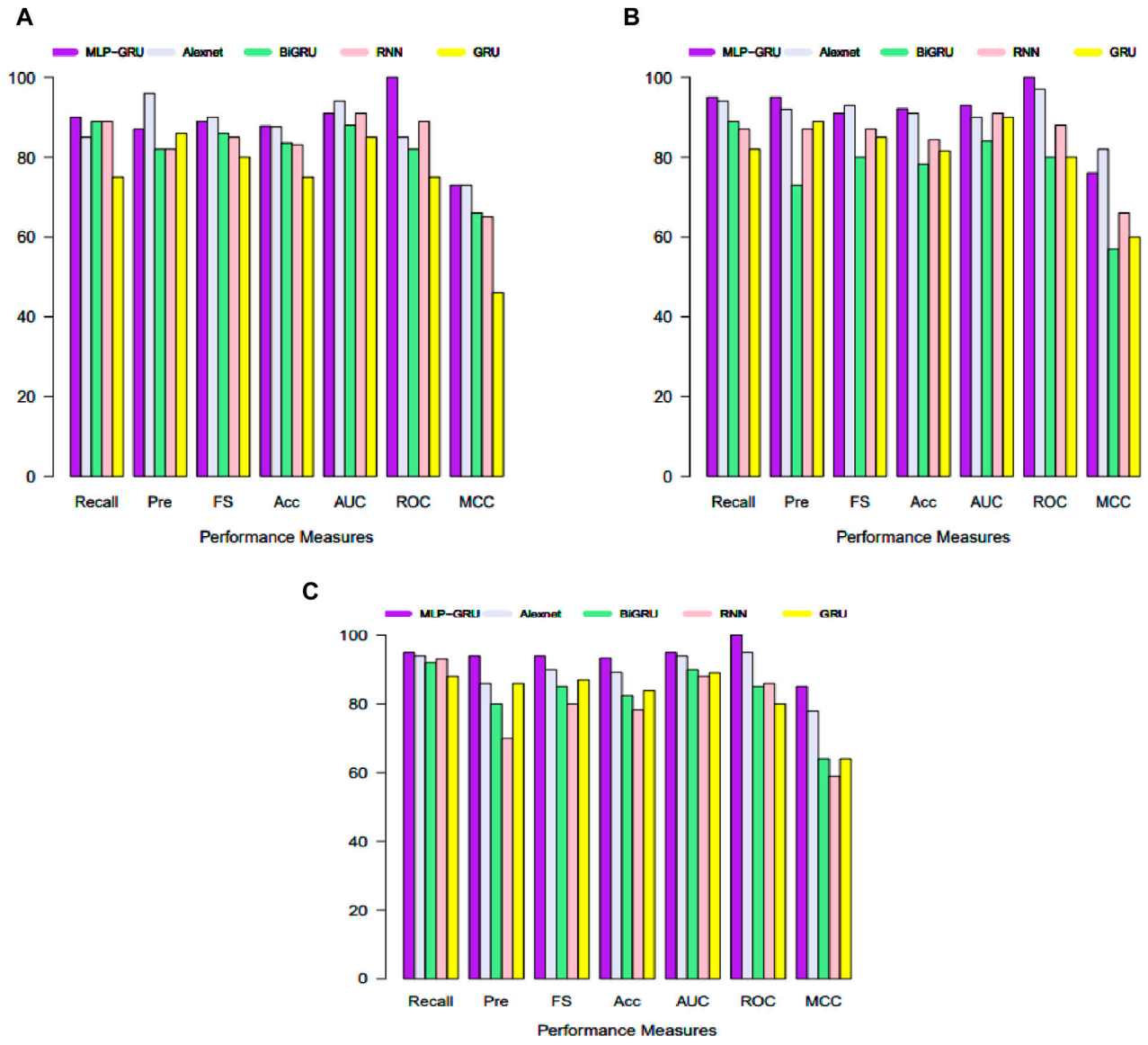

FIGURE 6
The performance measures bar plot for the proposed MPL-GRU vs. benchmark models with different training and testing datasets; **(A)** 50%, 50%, **(B)** 75%, 25%, and **(C)** 90%, 10%.

method used the current study dataset and computed the performance metrics [accuracy (89.9%), F-score (90.86%), and area under curve (78%)] that were also comparatively higher than our proposed system. On the other hand (Gul, 2020), reported the best-proposed approach for detecting electricity theft in the smart grid. For comparison, the authors obtained the evaluation measures for this approach, such as accuracy (91.29%), F1 score (90.96%), and area under the curve (0.87%), which were comparatively greater than the current proposed hybrid system. However, in the work (Bohani et al., 2021), the best-proposed method used the present study dataset and computed the performance indicators, that is, accuracy (91%), F1score (88.99%), and area under the curve (86%) that were also relatively higher than our proposed hybrid system. Also, the best-proposed model of (Razavi et al., 2019) was applied to this work's dataset, and their performance measures were obtained. The best-proposed model of (Meidan et al., 2020) reported the performance measures values as the following: accuracy = 57.70%, F-score = 70.01%, and area under curve = 77.01%, respectively, which are remarkably greater than our performance measures values: accuracy = 93.3%, F-score = 94.96%, and area under the curve = 95%. In a previous study (Pamir et al., 2022), the authors used the same dataset as our proposed hybrid system and achieved higher performance measures. For example, the accuracy, F1-score, and area under curve achieved by their best method were 73.20%, 70.10%, and 69.50%, respectively, which were significantly better than our proposed measures. Another study (Qu et al., 2020) also used our dataset and achieved higher accuracy (87.90%), F-score (96.11%), and area under the curve (87.90%) than our proposed hybrid system. In summary, our proposed hybrid system achieved high accuracy but was outperformed by the best methodologies in the literature.

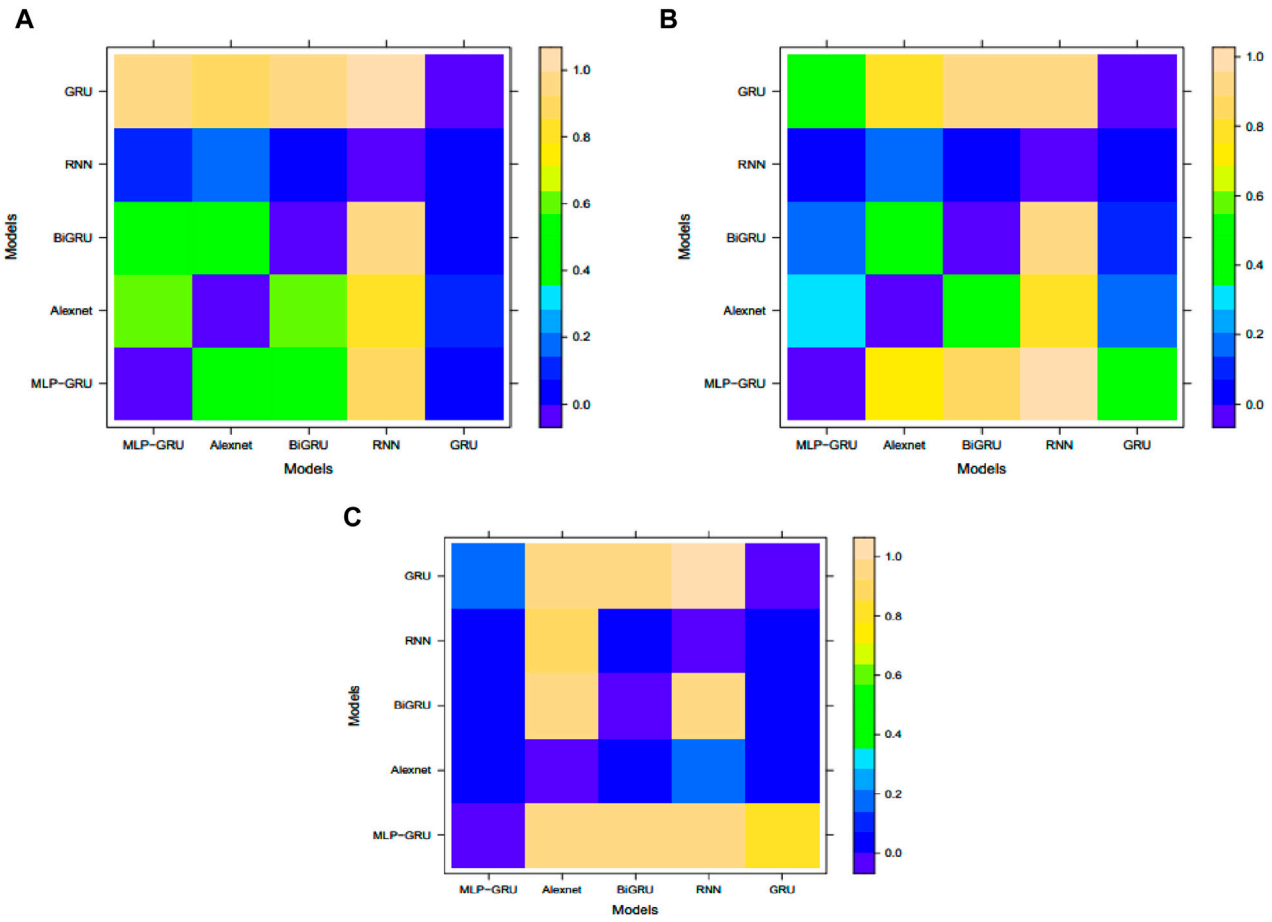

FIGURE 7
The level plots DMT results (*p*-values) for the proposed MPL-GRU vs. benchmark models with different training and testing datasets; **(A)** 50%, 50%, **(B)** 75%, 25%, and **(C)** 90%, 10%.

TABLE 7 The proposed work *versus* the related work performance indicator on CNGC data.

Technique	Data	Performance
The proposed model	CNGC	Recall = 95%, Precision = 97.5% F1-Score = 94% Accuracy = 93.33%, Test loss = 20% AUC = 95%, ROC = 100%, and MCC = 85%
Time and Location Gated Recurrent Unit (Pamir et al., 2022)	CNGC	Accuracy = 91%, Precision = 97.96%, and AUC = 91.68%
Wide and Deep Convolutional Neural (Zheng et al., 2017)	CNGC	AUC = 0.78, Mean Absolute Percentage Error = 0.90
SMOTE, LSTM (Qu et al., 2020)	CNGC	Accuracy = 0.89, Precision = 0.90, Recall = 0.87
SMOTE-LINK, Kernel, BGRU (Ramos et al., 2016)	CNGC	AUC = 0.86, Precision = 0.80, Recall = 0.89
CNN-LSTM (Hasan et al., 2019)	CNGC	Accuracy = 0.74, Precision = 0.725, recall = 0.85, F1-score = 0.779, ROC = 0.817
SVM (Toma et al., 2019)	CNGC	Accuracy = 0.577, Precision = 0.545, recall = 0.851, F1-score = 0.701, ROC = 0817
LR (Buzau et al., 2018)	CNGC	Accuracy = 0.732, Precision = 0.804, recall = 0.622, F1-score = 0.701, ROC = 0.645
LSTM (Adil et al., 2020)	CNGC	Accuracy = 0.879, Precision = 0.889, recall = 0.910, F1-score = 0.9611, ROC = 0.879

5 Conclusion

ETD is a significant issue in many countries, leading to a substantial financial loss for power utilities worldwide. However, conventional methods for ETD face challenges such as the curse of dimensionality and an imbalanced distribution of electricity consumption data. To overcome these problems, this study proposes a hybrid system named MLP-GRU that analyzes and

solves electricity theft using data from the CNGC. The proposed hybrid system consists of several steps. Firstly, the data undergoes preprocessing. Secondly, the k-means SMOTE technique is used to balance the data. Thirdly, the GRU model is applied to the extracted, purified data. Fourthly, the MLP model is also applied to the extracted, purified data. Finally, the performance of the proposed system is evaluated using various performance measures like a graphical analysis and a statistical test. To verify the consistency of the proposed hybrid system, the dataset is trained and tested using three different ratios. The study's results show that the proposed hybrid system for ETD is highly accurate and efficient compared to other models including Alexnet, GRU, BGRU and RNN. In our case, Hybrid MLP-GRU has solved complex nonlinear problem. It handles large amounts of input data and makes quick predictions after training. The same accuracy ratio can be achieved even with smaller samples.

The main advantage of this research is introducing an effective ETD model for power utilities, which enables them to minimize financial loss. Furthermore, the accurate and prompt detection of energy thieves decreases line losses in transformers and other grid components. The suggested model also has certain drawbacks. The model can only be trained using high-frequency data on electricity consumption, which restricts its ability to capture the minutest electricity consumption trends. Its accuracy was also reduced as a result, more cases of misclassification occur. Furthermore, there is no method for tweaking the hyper parameters, so it can take much computing time. In the future, we will improve its performance by using the minimum frequency dataset and decreasing the delay in identifying electricity theft in the CNGC dataset. Finally, the authors believe that the system proposed in this work can be extended to the ETD in other parts of the country and the world.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

HI: Writing–original draft, Writing–review and editing. NK: Writing–original draft, Writing–review and editing. MR: Writing–original draft, Writing–review and editing. GA: Writing–original draft, Writing–review and editing. MK: Writing–original draft, Writing–review and editing. MA: Writing–original draft, Writing–review and editing. ET: Writing–original draft, Writing–review and editing. AE: Writing–original draft, Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2024-1475-03".

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Adil, M., Javaid, N., Qasim, U., Ullah, I., Shafiq, M., and Choi, J. G. (2020). LSTM and bat-based RUSBoost approach for electricity theft detection. *Appl. Sci.* 10 (12), 4378. doi:10.3390/app10124378

Ahir, R. K., and Chakraborty, B. (2022). Pattern-based and context-aware electricity theft detection in smart grid. *Sustain. Energy, Grids Netw.* 32, 100833. doi:10.1016/j.segan.2022.100833

Alameady, M. H., Albermany, S., and George, L. E. (2022). Energy theft detection and preventive measures for IoT using machine learning. *Math. Statistician Eng. Appl.*, 7, 155–168.

Arif, A., Alghamdi, T. A., Khan, Z. A., and Javaid, N. (2022). Towards efficient energy utilization using big data analytics in smart cities for electricity theft detection. *Big Data Res.* 27, 100285. doi:10.1016/j.bdr.2021.100285

Asif, M., Nazeer, O., Javaid, N., Alkhammash, E. H., and Hadjouni, M. (2022). Data augmentation using BiWGAN, feature extraction and classification by hybrid 2DCNN and BiLSTM to detect non-technical losses in smart grids. *IEEE Access* 10, 27467–27483. doi:10.1109/access.2022.3150047

Aslam, Z., Ahmed, F., Almogren, A., Shafiq, M., Zuair, M., and Javaid, N. (2020). An attention guided semi-supervised learning mechanism to detect electricity frauds in the distribution systems. *IEEE Access* 8, 221767–221782. doi:10.1109/access.2020.3042636

Aziz, S., Hassan Naqvi, S. Z., Khan, M. U., and Aslam, T., (2020). Electricity theft detection using empirical mode decomposition and K-nearest neighbors, 2020 International Conference on Emerging Trends in Smart Technologies (ICETST). Karachi, Pakistan, IEEE.

Banga, A., Ahuja, R., and Sharma, S. (2022). Accurate detection of electricity theft using classification algorithms and Internet of Things in smart grid. *Arabian J. Sci. Eng.* 47 (8), 9583–9599. doi:10.1007/s13369-021-06313-z

Blazakis, K. V., Kapetanakis, T. N., and Stavrakakis, G. S. (2020). Effective electricity theft detection in power distribution grids using an adaptive neuro fuzzy inference system. *Energies* 13 (12), 3110. doi:10.3390/en13123110

Bohani, F. A., Suliman, A., Saripuddin, M., Sameon, S. S., Md Salleh, N. S., and Nazeri, S. (2021). A comprehensive analysis of supervised learning techniques for electricity theft detection. *J. Electr. Comput. Eng.* 2021, 1–10. doi:10.1155/2021/9136206

Buzau, M. M., Tejedor-Aguilera, J., Cruz-Romero, P., and Gomez-Exposito, A. (2018). Detection of non-technical losses using smart meter data and supervised learning. *IEEE Trans. Smart Grid* 10 (3), 2661–2670. doi:10.1109/tsg.2018.2807925

Buzau, M.-M., Tejedor-Aguilera, J., Cruz-Romero, P., and Gomez-Exposito, A. (2019). Hybrid deep neural networks for detection of non-technical losses in

electricity smart meters. *IEEE Trans. Power Syst.* 35 (2), 1254–1263. doi:10.1109/tpwrs.2019.2943115

Chandrasekhar, A., Vivekananthan, V., Khandelwal, G., Kim, W., and Kim, S. J. (2020). Green energy from working surfaces: a contact electrification–enabled data theft protection and monitoring smart table. *Mater. Today Energy* 18, 100544. doi:10.1016/j.mtener.2020.100544

Cheng, Q., Peng, B., Li, Q., and Liu, S., (2021). A rolling bearing fault diagnosis model based on WCNN-BiGRU, 2021 China automation congress (CAC). Beijing, China, IEEE.

Chung, J., Empirical evaluation of gated recurrent neural networks on sequence modeling. https://arxiv.org/abs/1412.3555, arXiv preprint arXiv:1412.3555, 2014.

de Souza, M. A., Pereira, J. L., Alves, G. d. O., de Oliveira, B. C., Melo, I. D., and Garcia, P. A. (2020). Detection and identification of energy theft in advanced metering infrastructures. *Electr. Power Syst. Res.* 182, 106258. doi:10.1016/j.epsr.2020.106258

Ding, N., Ma, H., Gao, H., Ma, Y., and Tan, G. (2019). Real-time anomaly detection based on long short-Term memory and Gaussian Mixture Model. *Comput. Electr. Eng.* 79, 106458. doi:10.1016/j.compeleceng.2019.106458

Duarte Soares, L., de Souza Queiroz, A., López, G. P., Carreño-Franco, E. M., López-Lezama, J. M., and Muñoz-Galeano, N. (2022). BiGRU-CNN neural network applied to electric energy theft detection. *Electronics* 11 (5), 693. doi:10.3390/electronics11050693

Fei, K., Li, Q., and Zhu, C. (2022). Non-technical losses detection using missing values' pattern and neural architecture search. *Int. J. Electr. Power & Energy Syst.* 134, 107410. doi:10.1016/j.ijepes.2021.107410

Gong, X., Tang, B., Zhu, R., Liao, W., and Song, L. (2020). Data augmentation for electricity theft detection using conditional variational auto-encoder. *Energies* 13 (17), 4291. doi:10.3390/en13174291

Gul, H., Detection of non-technical losses using sampling techniques and advance machine learning techniques to secure smart meters. https://www.researchgate.net/publication/374373661_Detection_of_non-technical_losses_using_sampling_techniques_and_advance_machine_learning_techniques_to_secure_smart_meters, 2020.

Gupta, A. K., Routray, A., and Naikan, V. A. (2022). Detection of power theft in low voltage distribution systems: a review from the Indian perspective. *IETE J. Res.* 68 (6), 4180–4197. doi:10.1080/03772063.2020.1787881

Hasan, M. N., Toma, R. N., Nahid, A. A., Islam, M. M. M., and Kim, J. M. (2019). Electricity theft detection in smart grid systems: a CNN-LSTM based approach. *Energies* 12 (17), 3310. doi:10.3390/en12173310

Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., and Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects. *Electronics* 11 (9), 1502. doi:10.3390/electronics11091502

Jaiswal, V. K., Singh, H. K., and Singh, K. (2020).Arduino gsm based power theft detection and energy metering , 5th international conference on communication and electronics systems (ICCES). Coimbatore, India, IEEE

Jindal, A., Dua, A., Kaur, K., Singh, M., Kumar, N., and Mishra, S. (2016). Decision tree and SVM-based data analytics for theft detection in smart grid. *IEEE Trans. Industrial Inf.* 12 (3), 1005–1016. doi:10.1109/tii.2016.2543145

Jokar, P., Arianpoo, N., and Leung, V. C. (2015). Electricity theft detection in AMI using customers' consumption patterns. *IEEE Trans. Smart Grid* 7 (1), 216–226. doi:10.1109/tsg.2015.2425222

Kabir, B., Pamir, Ullah, A., Munawar, S., Asif, M., and Javaid, N., (2021). Detection of non-technical losses using MLP-GRU based neural network to secure smart grids, Complex, Intelligent and Software Intensive Systems: Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2021). Cham, Germany. Springer.

Kabir, B., Qasim, U., Javaid, N., Aldegheishem, A., Alrajeh, N., and Mohammed, E. A. (2022). Detecting nontechnical losses in smart meters using a MLP-GRU deep model and augmenting data via theft attacks. *Sustainability* 14 (22), 15001. doi:10.3390/su142215001

Khalid, H. M., Muyeen, S., and Peng, J.C.-H. (2019). Cyber-attacks in a looped energy-water nexus: an inoculated sub-observer-based approach. *IEEE Syst. J.* 14 (2), 2054–2065. doi:10.1109/jsyst.2019.2941759

Khalid, H. M., Qasaymeh, M. M., Muyeen, S. M., Moursi, M. S. E., Foley, A. M., Sweidan, T. O., et al. (2023). WAMS operations in power grids: a track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks. *IEEE Syst. J.* 17, 3950–3961. doi:10.1109/jsyst.2023.3285492

Khan, N., (2024). A novel deep learning technique to detect electricity theft in smart grids using AlexNet. *IET Renewable Power Generation*. 17, 12846, doi:10.1049/rpg2.12846

Kocaman, B., and Tümen, V. (2020). Detection of electricity theft using data processing and LSTM method in distribution systems. *Sādhanā* 45 (1), 286. doi:10.1007/s12046-020-01512-0

Kumar, N., Singh, B., and Panigrahi, B. K. (2019). Grid synchronisation framework for partially shaded solar PV-based microgrid using intelligent control strategy. *IET Generation, Transm. Distribution* 13 (6), 829–837. doi:10.1049/iet-gtd.2018.6079

Kumar, N., Singh, B., and Panigrahi, B. K. (2022). Voltage sensorless based model predictive control with battery management system: for solar PV powered on-board EV charging. *IEEE Trans. Transp. Electrification* 9, 2583–2592. doi:10.1109/tte.2022.3213253

Kumar, N., Singh, B., Wang, J., and Panigrahi, B. K. (2020). A framework of L-HC and AM-MKF for accurate harmonic supportive control schemes. *IEEE Trans. Circuits Syst. I Regul. Pap.* 67 (12), 5246–5256. doi:10.1109/tcsi.2020.2996775

Kumari, P., Kumar, N., and Panigrahi, B. K. (2022). A framework of reduced sensor rooftop SPV system using parabolic curve fitting MPPT technology for household consumers. *IEEE Trans. Consumer Electron.* 69 (1), 29–37. doi:10.1109/tce.2022.3209974

Lepolesa, L. J., Achari, S., and Cheng, L. (2022). Electricity theft detection in smart grids based on deep neural network. *Ieee Access* 10, 39638–39655. doi:10.1109/access.2022.3166146

Li, W., Logenthiran, T., Phan, V. T., and Woo, W. L. (2019). A novel smart energy theft system (SETS) for IoT-based smart home. *IEEE Internet Things J.* 6 (3), 5531–5539. doi:10.1109/jiot.2019.2903281

Lowitzsch, J., Hoicka, C. E., and van Tulder, F. J. (2020). Renewable energy communities under the 2019 European Clean Energy Package–Governance model for the energy clusters of the future? *Renew. Sustain. Energy Rev.* 122, 109489. doi:10.1016/j.rser.2019.109489

Meidan, Y., Sachidananda, V., Peng, H., Sagron, R., Elovici, Y., and Shabtai, A. (2020). A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Comput. Secur.* 97, 101968. doi:10.1016/j.cose.2020.101968

Mukhopadhyay, R., (2019). "Model learning for robotic manipulators using recurrent neural networks," in TENCON 2019-2019 IEEE Region 10 Conference (TENCON) Kochi, India, (IEEE).

Munawar, S., Asif, M., Kabir, B., Pamir, Ullah, A., and Javaid, N., (2021). Electricity theft detection in smart meters using a hybrid bi-directional GRU bi-directional LSTM model, Complex, Intelligent and Software Intensive Systems: Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2021). Cham, Germany, Springer

Muzumdar, A., Modi, C., and Vyjayanthi, C. (2022). Designing a blockchain-enabled privacy-preserving energy theft detection system for smart grid neighborhood area network. *Electr. Power Syst. Res.* 207, 107884. doi:10.1016/j.epsr.2022.107884

Østergaard, P. A., Duic, N., Noorollahi, Y., and Kalogirou, S. A. (2021). Recent advances in renewable energy technology for the energy transition. *Elsevier* 179, 877–884. doi:10.1016/j.renene.2021.07.111

Pamir, Javaid, N., Javaid, S., Asif, M., Javed, M. U., Yahaya, A. S., et al. (2022). Synthetic theft attacks and long short term memory-based preprocessing for electricity theft detection using gated recurrent unit. *Energies* 15 (8), 2778. doi:10.3390/en15082778

Park, C. H., and Kim, T. (2020). Energy theft detection in advanced metering infrastructure based on anomaly pattern detection. *Energies* 13 (15), 3832. doi:10.3390/en13153832

Qu, Z., Li, H., Wang, Y., Zhang, J., Abu-Siada, A., and Yao, Y. (2020). Detection of electricity theft behavior based on improved synthetic minority oversampling technique and random forest classifier. *Energies* 13 (8), 2039. doi:10.3390/en13082039

Quasim, M. T., Nisa, K. u., Khan, M. Z., Husain, M. S., Alam, S., Shuaib, M., et al. (2023). An internet of things enabled machine learning model for Energy Theft Prevention System (ETPS) in Smart Cities. *J. Cloud Comput.* 12 (1), 158. doi:10.1186/s13677-023-00525-4

Rahman, M. M., Oni, A. O., Gemechu, E., and Kumar, A. (2020). Assessment of energy storage technologies: a review. *Energy Convers. Manag.* 223, 113295. doi:10.1016/j.enconman.2020.113295

Ramos, C. C., Rodrigues, D., de Souza, A. N., and Papa, J. P. (2016). On the study of commercial losses in Brazil: a binary black hole algorithm for theft characterization. *IEEE Trans. Smart Grid* 9 (2), 676–683. doi:10.1109/tsg.2016.2560801

Razavi, R., Gharipour, A., Fleury, M., and Akpan, I. J. (2019). A practical feature-engineering framework for electricity theft detection in smart grids. *Appl. energy* 238, 481–494. doi:10.1016/j.apenergy.2019.01.076

Rehan, M., Raza, M. A., Aman, M., Abro, A. G., Ismail, I. M. I., Munir, S., et al. (2023). Untapping the potential of bioenergy for achieving sustainable energy future in Pakistan. *Energy* 275, 127472. doi:10.1016/j.energy.2023.127472

Ren, S., Hao, Y., Xu, L., Wu, H., and Ba, N. (2021). Digitalization and energy: how does internet development affect China's energy consumption? *Energy Econ.* 98, 105220. doi:10.1016/j.eneco.2021.105220

Saxena, V., Kumar, N., Singh, B., and Panigrahi, B. K. (2021). An MPC based algorithm for a multipurpose grid integrated solar PV system with enhanced power quality and PCC voltage assist. *IEEE Trans. Energy Convers.* 36 (2), 1469–1478. doi:10.1109/tec.2021.3059754

Siu, J. Y., Kumar, N., and Panda, S. K. (2022). Command authentication using multiagent system for attacks on the economic dispatch problem. *IEEE Trans. Industry Appl.* 58 (4), 4381–4393. doi:10.1109/tia.2022.3172240

Stracqualursi, E., Rosato, A., Di Lorenzo, G., Panella, M., and Araneo, R. (2023). Systematic review of energy theft practices and autonomous detection through artificial

intelligence methods. *Renew. Sustain. Energy Rev.* 184, 113544. doi:10.1016/j.rser.2023.113544

Toma, R. N., Hasan, M. N., Nahid, A. A., and Li, B. (2019). Electricity theft detection to reduce non-technical loss using support vector machine in smart grid, 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). Dhaka, Bangladesh, IEEE

Ullah, A., Javaid, N., Asif, M., Javed, M. U., and Yahaya, A. S. (2022). Alexnet, adaboost and artificial bee colony based hybrid model for electricity theft detection in smart grids. *Ieee Access* 10, 18681–18694. doi:10.1109/access.2022.3150016

Xie, R. (2023).An energy theft detection framework with privacy protection for smart grid. 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, IEEE.

Xu, C., Shen, J., Du, X., and Zhang, F. (2018). An intrusion detection system using a deep neural network with gated recurrent units. *IEEE Access* 6, 48697–48707. doi:10.1109/access.2018.2867564

Zhang, Y., Ai, Q., Wang, H., Li, Z., and Zhou, X. (2020). Energy theft detection in an edge data center using threshold-based abnormality detector. *Int. J. Electr. Power & Energy Syst.* 121, 106162. doi:10.1016/j.ijepes.2020.106162

Zheng, Z., Yang, Y., Niu, X., Dai, H. N., and Zhou, Y. (2017). Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. *IEEE Trans. Industrial Inf.* 14 (4), 1606–1615. doi:10.1109/tii.2017.2785963

Zidi, S., Mihoub, A., Mian Qaisar, S., Krichen, M., and Abu Al-Haija, Q. (2023). Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. *J. King Saud University-Computer Inf. Sci.* 35 (1), 13–25. doi:10.1016/j.jksuci.2022.05.007

Nomenclature

(ETD)	Electricity Theft Detection
(MLP)	Multi-Layer Perceptron
(GTU)	Gated Recurrent Units
(CNGC)	Chinese National Grid Corporation
(SMOTE)	Synthetic Minority Oversampling Technique
(BGRU)	Bidirectional Gated Recurrent Unit
(RNN)	Recurrent Neural Network
(TL)	Technical Losses
(NTLs)	Non-Technical Losses
(UK)	United Kingdom
(USA)	United States of America
(AMI)	Advanced Metering Infrastructure
(RF)	Random Forest
(DT)	Decision trees
(BE)	Bagging Ensemble
(ANN)	Artificial Neural Networks
(KNN)	K-Nearest Neighbors
(NAS)	Neural Architecture Search
(AUC)	Area Under the Curve
(LSTM)	Long Short-Term Memory
(CNN)	Convolutional Neural Networks
(Bi-LSTM)	Bidirectional Long Short-Term Memory
(2D-CNN)	Two-Dimensional Convolutional Neural Networks
(ABC)	Artificial bee Colony
(DNN)	Deep Neural Network
(IoT)	Internet of Things
(SVM)	Support Vector Machine
(CVAE)	Conditional Variation Auto-Encoder
(IoT)	Internet of Things
(DoS)	Denial-of-Service
(DDoS)	Distributed Denial-of-Service
(U2R)	User-to-Root
(R2L)	Remote-to-Local
(MITM)	Man-in-the-Middle
(WAMS)	Wide Area Monitoring System
(MDML)	Mixture Density-based Maximum Likelihood
(TLF)	Track-Level Fusion
(MPI)	Message Passing Interface
(TBSSVM)	Technique with Support Vector Machine
(TCN-EMLP)	Temporal Convolutional Network with Enhanced Multi-Layer Perceptron
(GMM)	Gaussian Mixture Model
(SI)	Simple Imputer
(ReLU)	Rectified Linear Unit
(LSTM)	Long Short-Term Memory
(MCC)	Matthews' correlation coefficient
(TP)	True Positive
(TN)	True Negative
(FP)	False Positive
(FN)	False Negative
(TPR)	True Positive Rate
(FDR)	Fraud Detection Rate
(DMT)	Diebold and Mariano Test.